RFC 2631 Diffie-Hellman Key Agreement Method

References:

```
RFC 2631, Diffie-Hellman Key Agreement Method
[X942],   Agreement Of Symmetric Keys Using Diffie-Hellman
          and MQV Algorithms, ANSI draft, 1998
```

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/ na)	NOTES
In the process of generating keying material from ZZ: KM = H (ZZ || OtherInfo), where ZZ = (yb ^ xa) mod p = (ya ^ xb) mod p (^ denotes exponentiation) and ya is party a's public key; ya = g ^ xa mod p yb is party b's public key; yb = g ^ xb mod p xa is party a's private key xb is party b's private key p is a large prime q is a large prime g = h^{(p-1)/q} mod p, where h is any integer with 1 < h < p-1 such that h{(p-1)/q} mod p > 1 (g has order q mod p; i.e. g^q mod p = 1 if g!=1) j a large integer such that p=qj + 1 are the leading zeros of ZZ preserved, so that ZZ occupies as many octets as p? [RFC 2631 2.1.1, 2.1.2, X942]		
For the OtherInfo parameter used to generate keying material, if the partyAInfo field is provided, does it contain 512 bits? [RFC 2631 2.1.2]		

REQUIREMENT FROM STANDARDS	MET (Y/N/ na)	NOTES
For the OtherInfo parameter used to generate keying material, is the partyAInfo parameter used in Static-Static mode? [RFC 2631 2.1.2]		
When the KEK is generated for 3DES, is the algorithm run twice, once with a counter value of 1 (to generate K1', K2', and the first 32 bits of K3') and once with a counter value of 2 (to generate the last 32 bits of K3)? [RFC 2631 2.1.3]		
For the group parameters of the form p=jq + 1 where q is a large prime of length m and j>=2, is m >=160 bits in length? [RFC 2631 2.2]		
For the group parameters of the form p=jq + 1 where q is a large prime of length m and j>=2, is q at least 160 bits long? [RFC 2631 2.2]		
For the group parameters of the form p=jq + 1 where q is a large prime of length m and j>=2, is p a minimum of 512 bits long? [RFC 2631 2.2]		
If the same ephemeral sender key is used for multiple messages (e.g., it is cached as a performance optimization) then is a separate partyAInfo used for each message? [RFC 2631 2.3]		
Do all mechanisms implement Ephemeral-Static mode? [RFC 2631 2.3]		
In the Static-Static mode, is the parameter partyAInfo used (and different for each message) in order to ensure that different messages use different KEKs? [RFC 2631 2.4]		

Other information:

Findings:

Recommendations for Standards Work: